Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims:

Claim 1. (currently amended) A method of decrypting encrypted content stored on a terminal, the method comprising the steps of:

receiving a request to access encrypted content on a terminal;

obtaining a license comprising a content decryption key and a set of binding attributes, the attributes including a public key of an authorized user of the encrypted content;

in response to the request, polling a personal trusted device of said user to digitally sign data with a private key associated with the device;

~~establishing communication link between the terminal and at least one other terminal; and~~

receiving said digitally signed data from said device~~on the communication link at the terminal from the other terminal~~;

verifying at the terminal the digitally signed data utilizing the ~~said~~ public key; and wherein the terminal in response to verification of the digitally signed data uses the content decryption key to decrypt the encrypted content.

Claim 2. (original) A method as claimed in claim 1, comprising: encrypting at least the content decryption key.

Claim 3. (original) A method as claimed in claim 2, wherein: encryption is performed using a public key of an asymmetric key pair such that decryption of the content decryption key

is carried out using a private key of the asymmetric key pair.

Claim 4. (original) A method as claimed in claim 3, wherein: the private key is stored in a tamperproof and secure location.

Claim 5. (original) A method as claimed in claim 4, wherein: the secure location comprises a security element.

Claim 6. (currently amended) A computer readable medium storing computer executable instructions for performing ~~program comprising: executable code which executes when loaded on a computer, to perform~~ the method according to claim 1.

Claim 7. (currently amended) A computer readable medium storing computer executable instructions for performing ~~program comprising: executable code which executes when loaded on a computer, to perform~~ the method according to claim 2.

Claim 8. (currently amended) A computer readable medium storing computer executable instructions for performing ~~program comprising: executable code which executes when loaded on a computer, to perform~~ the method according to claim 3.

Claim 9. (currently amended) A computer readable medium storing computer executable instructions for performing~~program comprising: executable code which executes when loaded on~~

~~a computer, to perform~~ the method according to claim 4.

Claim 10. (currently amended) A computer readable medium storing computer executable instructions for performing ~~program comprising: executable code which executes when loaded on a computer, to perform~~ the method according to claim 5.

Claims 11-15. (canceled)

Claim 16. (currently amended) A terminal which renders encrypted content comprising:

a storage for the encrypted content and a license, the license containing a content decryption key and a set of binding attributes, the attributes including a public key for a licensee of said content;

a protected processing environment;

a network interface which, in response to said terminal receiving a request to access said stored encrypted content, establishes a communication link between the terminal and at least one other terminal to request the other terminal to encrypt and digitally sign identity verification data using a private key stored at the other terminal, and which delivers the digitally signed identity verification data received from the other terminal to the protected processing environment; and

wherein the protected processing environment uses said public key to decrypt said encrypted identity verification data, compares said decrypted data with said digital signature to verify the digitally signed data, and upon successful verification of the digitally signed data, ~~with the public key,~~ the protected processing environment decrypts the encrypted content using the

content decryption key.

Claim 17. (original) A terminal as claimed in claim 16, comprising: a tamperproof and secure storage for a private key of an asymmetric key pair; and wherein the protected processing environment decrypts at least the content decryption key, the content decryption key having been encrypted using a public key of the asymmetric key pair.

Claim 18. (original) A terminal as claimed in claim 17, wherein: the storage is provided by a security element.

Claim 19. (currently amended) A terminal as claimed in claim 16, wherein: the digitally signed identity verification data is delivered to the storage.

Claim 20. (currently amended) A terminal as claimed in claim 17, wherein: the digitally signed identity verification data is delivered to the storage.

Claim 21. (currently amended) A terminal as claimed in claim 18, wherein: the digitally signed identity verification data is delivered to the storage.

Claim 22. (currently amended) A terminal as claimed in claim 16, wherein: the protected processing environment verifies the digitally signed identity verification data.

Claim 23. (currently amended) A terminal as claimed in claim 17, wherein: the protected processing environment verifies the digitally signed identity verification data.

Claim 24. (currently amended) A terminal as claimed in claim 18, wherein: the protected processing environment verifies the digitally signed identity verification data.

Claim 25. (currently amended) A terminal as claimed in claim 19, wherein: the protected processing environment verifies the digitally signed identity verification data.

Claim 26. (currently amended) A terminal as claimed in claim 20, wherein: the protected processing environment verifies the digitally signed identity verification data.

Claim 27. (currently amended) A terminal as claimed in claim 21, wherein: the protected processing environment verifies the digitally signed identity verification data.

Claims 28-71 (canceled)

Claim 72. (currently amended) A terminal which renders encrypted content comprising:

a storage for the encrypted content and a license, the license containing a content decryption key and a set of binding attributes, the attributes including a public key;

a protected processing environment;

a communication link between the terminal and at least one other terminal which delivers digitally signed data from the other terminal to the terminal;

a digital rights management engine disposed in a non-secure part of the terminal; ~~and~~

a digital rights management agent disposed within the protected processing environment which verifies if the digitally signed data is signed by a licensee of the encrypted content and upon verification, uses the content decryption key to decrypt the encrypted content;

wherein the storage is unprotected, the digital rights management engine decrypts the set of binding attributes to determine if the encrypted content is licensed to the licensee to be decrypted and if the encrypted content is authorized to be decrypted signals the digital rights management engine to render the content; the decryption key is encrypted; and the digital rights management agent obtains the binding attributes and obtains the content decryption key by using a private protected processing environment key to decrypt the encrypted decryption key.

Claim 73-75. (canceled)

Claim 76. (original) A terminal in accordance with claim 72 wherein: an encrypted part of the license includes a user identity certificate issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

Claim 77. (currently amended) A terminal in accordance with claim ~~74~~ 72 wherein: an encrypted part of the license includes a user identity certificate issued and digitally signed by a

certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

Claim 78. (original) A terminal in accordance with claim 72 wherein: an encrypted part of the license includes a URL which is an address at which a user identity certificate was issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

Claims 79-81. (canceled)

Claim 82. (currently amended) A terminal in accordance with claim 76 wherein: an encrypted part of the license includes a URL which is an address at which a user identity certificate issued and digitally signed by a certification authority ~~may be~~is obtained which permits a licensor of the content to establish a level of trust in a licensee of the content.

Claim 83. (original) A terminal in accordance with claim 77 wherein: an encrypted part of the license includes a URL which is an address at which a user identity certificate was issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

Claim 84 (new) The method of claim 1, wherein said personal trusted device is a mobile telephone.

Claim 85 (new) The method of claim 1, wherein said personal trusted device is communicatively coupled with said terminal via a wireless interface.

Claim 86 (new) The method of claim 85, wherein said wireless interface is a low power radio frequency interface.

Claim 87 (new) The method of claim 1, wherein said terminal is a rendering machine, and said method further includes a step of rendering said decrypted content on said rendering machine.

Claim 88 (new) The method of claim 1, further comprising the steps of:

receiving an identification of a user making said request; and

comparing said identification with a public portion of said license.

Claim 89 (new) The method of claim 88, further comprising the step of accessing public portions of a plurality of licenses stored on said terminal to locate a license corresponding to said user.

Claim 90 (new) The method of claim 1, further comprising the step of randomly

generating textual data to be signed by said device.

Claim 91 (new) The method of claim 90, wherein said step of randomly generating is performed by said device.

Claim 92 (new) The method of claim 1, further comprising the steps of:

following said step of receiving said digitally signed data, applying a hashing algorithm to both said data and a signature of said digitally signed data; and

comparing results of said applications of said hashing algorithm in said step of verifying.

Claim 93 (new) The terminal of claim 16, wherein said identity verification data is a text string randomly generated by said other terminal.

Claim 94 (new) The terminal of claim 16, wherein said other terminal is a mobile telephone of said licensee.